Track 5: Global strategy, organization and value chains
Session format: competitive

The Internet of Things and its Implications for International Business Theory

Abstract: While the Internet of Things (IoT) has been seen to provide a global network infrastructure facilitating cross-border flow of goods and information, much of the current discussion focuses rather on consumer applications, leaving its implications for global businesses underexplored. We believe that the IoT has the potential to reconfigure industry structure and particularly global value chains. In this article, we map out the benefits of the Internet of Things to firms and to industries, whilst drawing attention to numerous constraints, including a Sino-US technology race, that may prohibit the realization of these benefits for developing country firms. Furthermore, we reflect on how the Internet of Things may pose new questions to international business theory, with a particular focus on internalization decisions, as well as drawing on the thriving ecosystem perspective. Our discussion culminates with the dark side of the Internet of Things which could amplify the asymmetric power relationships already observed in global value chains.

Keywords: digital technology; internet of things; global value chain; internalization; ecosystem

Introduction

The Internet of Things (IoT) has been conceptualized (Lu et al., 2018) as "a dynamic global network infrastructure that will be integrated into and act as an extension of the future internet, in which various "*things*" have unique identities, physical attributes, virtual personalities, and intelligent interfaces." The IoT involves an increasing number of smart, connected products being equipped with sensors that are able to collect and process information, and to then communicate that information in real-time to people and other products. As Fleisch (2010: 5) comments, "the IoT is all about sensing the physical world…. It is a cost-efficient means of growing a very finely granulated nerve system with trillions of new nerve endings. Linked together, they can provide humans with a measurement tool that opens the door to many new findings, applications, benefits, and risks." Importantly for international business practice and theory, the IoT has the potential to become a global network infrastructure, transcending national boundaries and facilitating cross-border transactions and flows of information.

A notable implication is that the IoT may bring fundamental improvements in the location and control of geographically-dispersed global value chains (GVCs). Presently, most firms monitor flows of physical products, and also maintain separate flows of information. In an IoT-enabled world, products will be assigned unique identifiers, and will be inextricably linked to information about their specifications, provenance, and end destination. There will no longer be a requirement to coordinate and synchronise product and information flows. This conflation will potentially give rise to substantial benefits in production and distribution efficiency, and particularly so when cross-border flows within GVCs are involved. We might thus expect the advent of the IoT to reduce the transaction costs associated with international production, and to facilitate an ever-deeper international division of labour (Strange & Zucchella, 2017). However, to better understand what the IoT would bring to the realm of international business requires a more comprehensive reflection on how the technology might change some of the parameters, and hence predictions, of the conventional theory.

In this paper, we consider how IoT deployment may generate value and bring benefits to firms, to consumers, and to society. These potential benefits include not only user gains in the form of more personalized products and greater convenience, but also efficiency gains, preventative maintenance, user feedback, and new business applications for firms. Next, we consider possible practical constraints on the realization of these benefits, particularly in the context of GVC activities undertaken in developing/emerging economies. These constraints include issues related to 5G connectivity, architecture standards, the availability of human resources, trust, security and data privacy. The penultimate section discusses the implications of IoT deployment for international business (IB) practice and theory focusing, in particular, on the decision about which GVC activities are best internalized (integrated) and which are best externalized (outsourced) and on how IoT may advance the perspective of ecosystems vis-à-vis the market/hierarchy bifurcation in international business research (Li et al., 2019). Our core message revolves around the dark side of the Internet of Things, highlighting the asymmetric power relationships within GVCs (Strange & Humphrey, 2018). The final section concludes and offers some suggestions for future research. We maintain that it is imperative for IB research to concern itself with the emergence of the IoT, if IB seeks to remain relevant to global businesses facing inevitable digitization. This paper infuses timely insights into the recent debate on how widespread technological transformation in the digital era poses new questions and opportunities to international business scholarship (Banalieva & Dhanaraj, 2019; Coviello et al., 2017; Li et al., 2019).

IoT and the Technology

IoT systems involve three main technological layers (i.e. devices, gateways, and service platforms), which together constitute the “technology stack” (see Figure 1). The technology stack embraces a range of technologies, standards, and applications which lead from the simple connection of products to complex applications that use the data that are captured in an accurate, secure and cost-effective manner. The first layer consists of a range of devices (e.g. sensors, actuators, transceivers) that are embedded in the products (cars, machinery, buildings etc), and which make the products smart. Sensors are fitted with radio-frequency identification (RFID), and detect and measure various environmental parameters (e.g. location, proximity, temperature, humidity, throughput, wear-and-tear, energy usage), and convert this data into electrical signals. Often these data are collected for analysis (see below), but sometimes the signals are received by actuators that trigger appropriate responses in the physical world (e.g. cooling down a machine whose temperature is too hot). These devices are responsible for capturing and transmitting the information, and a smart product may contain a few such devices or thousands. The second layer involves the IoT gateway, which consists of both hardware and software. The essential function of the gateway is internet connectivity, i.e. to provide a bridge between the devices (where data are captured) and the platforms (where the data are analysed). The gateway thus manages the devices, enables remote monitoring, pre-processes and aggregates the data, encrypts and decrypts the data (security), and specifies and translates the protocols that enable communications between the products and the platforms. IoT gateway devices and solutions come in many shapes and forms: some (typically those used for consumer applications) are fairly standard, whilst the functions and features of others (typically those used for differentiated industrial applications) need to be customized to the individual application. In terms of security, the gateway means that the devices are not directly connected to the outside world, from where most threats would arise. The third layer consists of the service platforms, which may reside on a local network, in a data centre, or in the cloud. These platforms offer some combination of the following capabilities: management of IoT devices and connectivity; access, ingestion, and processing of data; visualization and analysis of data; and application development and integration. Platforms are all about the generation of user benefits. Such platforms harness the data from the devices, and turn that data into useful business outcomes. It is important to note that standard IoT devices, gateways, and platforms are already (at the time of writing) available from specialised vendors, but that issues of standardization and inter-operability are still problematic.

The Benefits of IoT Deployment

Much has been written in the academic literature and elsewhere about the potential benefits of widespread IoT deployment for firms and for consumers. These benefits involve improvements in value-chain efficiency, performance monitoring, constructive responses to user feedback, and collection of data to enhance marketing efforts.

First, IoT adoption has the potential to facilitate the coordination of value-chains, and particularly globally-dispersed GVCs, and thus improve the operational efficiency of the chains. Operating costs may be reduced through enhanced automation, reduced labour costs, better inventory management, improved tracking and tractability, and the avoidance of materials being lost (Porter & Heppelmann, 2015; Leminen, 2018). Furthermore, as Fleisch (2010: 14) comments, the “IoT, with its technologies to automate the bridging of the last mile between the Internet and the physical world, dissolves the transaction costs that are caused by real world-virtual world media breaks. A real world-virtual world media break occurs when a piece of information is transferred from one carrier medium (e.g. a bar code) to another (e.g. a database that serves a warehouse management system). When things become computers, these media breaks, along with their attached costs, fade away.” Second, smart products can monitor and report on their own condition, performance and environment, helping to generate insights into their use and allow for preventative maintenance and/or remedial actions (Bughin et al., 2015; Porter & Heppelmann, 2015). In principle, this should allow production and energy costs to be reduced, and the costs/delays associated with system downtimes to be avoided. Third, IoT adoption allows firms to obtain detailed feedback via the smart products from their users/customers. This enables them to customise the products for individual users, offer additional services, optimise the product experience to individual needs, and build up customer loyalty (Fleisch, 2010). For the users, this translates into a more personalized and valuable purchasing experience: whether the enhanced value of this experience is retained by the user, or captured by the firm through higher prices is another matter! Fourth, this user feedback also allows firms to collect (big) data on users' needs and demands, and hence tailor their future marketing accordingly and develop new business applications (Porter & Heppelmann, 2014; Porter & Heppelmann, 2015; Ehret & Wirtz, 2017; Woodside & Sood, 2017; Leminen, 2018; Osmonbekov & Johnston, 2018; Zucchella et al., 2019)[1]. As Bhatia et al (2019: 4-5) comment, many firms "are moving in several ways to generate value from IoT beyond basic cost and efficiency plays. Some are generating additional revenue streams by offering IoT-supported services to their customers… Other companies are using IoT to discover their customer preferences…. Companies are also using IoT to enhance the customer experience… IoT products are also helping improve safety and wellness."

The Constraints on IoT Deployment

In this section, we briefly discuss various potential constraints on IoT adoption encountered by firms, with a focus on the likely problems to be met in developing/emerging

[1] De Cremer et al (2017) discuss the "dark side of the IoT", or the dubious practices that firms can use to exploit their customers. They conclude that the IoT provides firms with power in terms of data-driven knowledge, and this allows them greater potential for the exploitation of ever-more-powerless customers.

economies: poor Internet connectivity; the absence of internationally-recognised standards for IoT architecture; the unavailability of labour resources with the necessary skills; a lack of trust; and concerns about cyber-security and data protection.

First, the widespread and successful deployment of the IoT depends crucially upon the availability of fifth-generation (5G) telecommunications technology to connect devices to the internet. Earlier technologies were designed for communication between people[2], but 5G technology will allow mass connectivity between *things* and will thus act as a gateway for the IoT (Vella, 2019). This is because 5G technology uses much higher radio frequencies (30-300 GHz compared to 6GHz in the past) to transfer significantly more data over the air. This higher-frequency spectrum that 5G networks will use has a number of advantages (see Table 1):

Greater capacity: A wider radio spectrum implies more greater network capacity. 5G will be able to support many more devices (~ 1m devices per km^2) than 4G, hence there will be less congestion.

Faster speeds: bandwidth refers to the maximum amount of data that can be moved (uploaded or downloaded) over a network during a given period of time. 4G has a bandwidth of 200 megabits per second (mbps), whilst 5G promises a bandwidth in excess of 1 gigabit per second. Normal speeds vary according to a number of factors (including *inter alia* the number of devices on the network, interference, and whether the devices are moving or not), but will generally be lower than the bandwidth. But it is realistic to assume that average 5G speeds will be at least ten times faster than 4G speeds.

Reduced latency: latency refers to the time between an instruction is issued and data transfer is carried out, and low latency is essential when controlling devices in real-time. Latency in 4G networks is about 20-30 milliseconds, but this should fall to about 1-4

[2] Second-generation (2G) technology was introduced in the early 1990s, and allowed text and picture messaging. Third-generation (3G) technology came in the early 2000s, and permitted smartphones to run apps and access the internet. Fourth-generation (4G) technology arrived about a decade later, and was essentially a faster version of 3G.

milliseconds in 5G networks. This improvement is not just about speed of response, but also about performance in the sense of autonomous products being able to adjust almost instantaneously to changing conditions.

Reduced interference: 5G relies on a new digital technology (Massive MIMO) that is highly directional, and can be used next to other without causing interference. In contrast, the technology used by 4G beams radio waves in all directions, and uses more energy in so doing.

Table 1: Comparison of 3G, 4G and 5G Technologies

	3G	**4G**	**5G**
Deployment	Early 2000s	Early 2010s	2020 onwards
Radio frequencies		6 GHz	30-300 GHz
Capacity (devices)		~ 4000 / km^2	~ 1 million / km^2
Bandwidth	2 mbps	200 mbps	> 1gbps
Average speeds	144 kbps	10 mbps	100 mbps
Latency	100-500 millisecs	20-30 millisecs	1-4 millisecs

Sources: Vella (2019) and other sources

The roll-out of the 5G network will involve considerable capital investment. Massive MIMO and 5G New Radio will need to be installed at network base stations on top of the existing 4G infrastructure (Vella, 2019). Furthermore, the high-frequencies used by 5G not only require direct line-of-sight between the antenna and the device receiving the signal., but the signals do not travel very far. This will necessitate the installation of many more strategically-placed antennae, and also repeating stations to provide long-range 5G support. The availability of 5G will thus be an evolutionary process: South Korea, China, Japan and the United States appear to be in vanguard of this process and roll-out in urban areas will start from 2020, with other developed countries close behind (Vella, 2019). In addition, local networks may allow coverage for individual IoT applications. But the scale and cost of the capital investments mean that private network operators are unlikely to make the necessary infrastructure improvements in rural areas and/or low-income regions[3], unless subsidized by local/national governments (Chiaraviglio et al., 2017). This suggests that 5G roll-out may well be more of a reality in advanced countries than in many developing countries.

The IoT extends the Internet into the physical world and functions within the existing Internet infrastructure (Lu et al., 2018). A second constraint on IoT deployment relates to inter-operability, and the fact that the growing interconnectivity of smart products, gateways, platforms, machines and people will require new international standards that guide the interaction of these elements in global value chains (Rüβmann et al., 2015). Weyrich & Ebert (2016: 116) review various recent initiatives towards the development of reference architectures for the IoT in order to "avoid systems that are crippled because they can't talk with each other." Fleisch (2010: 7-8) comments that "there is currently no single global set of standards for the IoT and, in all likelihood, there never will be". However, he does acknowledge the emergence of *de facto* standards in certain industries (e.g. retail and consumer goods). Perhaps a more intractable obstacle will be provided by the geopolitical ambitions of China and the West in terms of 5G connectivity. Capri (2018) reports that China is not only deploying its version of 5G technology in its home market, but is also rolling it out in countries embraced by the Belt & Road Initiative. Meanwhile, foreign firms (including Ericsson, Samsung, Qualcomm, NTT Docomo) are deploying their own proprietary technology in their countries. Both sides are lobbying the Institute of Electrical and Electronics Engineers (IEEE) and other standards-setting organizations. Capri (2018) suggests that harmonized 5G standards and protocols might eventually materialize, but considers that a Sino-US technology race makes it more likely that a fragmented 5G landscape will emerge with different blocs coalescing around different interests. He (Capri, 2018) concludes that this "puts multinational companies in the position of having to craft business strategies to manage different standards, different threats

[3] Such regions include both areas of low population density, and areas where per capita incomes are low.

and different regulations from one region to the next. This adds complexity and costs to global operations, and, by having to ring-fence off China-focused businesses, multinationals will have to grapple with disrupted value chains - in addition to the threat of being whipsawed by new U.S. sanctions."

Third, technology availability is not by itself sufficient to realize the potential benefits: firms must also have the capacity to capitalize on the opportunities offered by the new technologies. Smart products, gateways and platforms may be general purpose technologies (Campbell et al., 2017), but they will all need to be customized, programmed, and installed for particular user applications, and the resultant data analysed. This will require a labour force[4] skilled in areas such as systems engineering, machine learning, software design, data analytics, and associated managerial roles (Chen et al., 2012; Porter & Heppelmann, 2014; Gupta & George, 2016; Kenney & Zysman, 2019). As Weyrick & Ebert (2016: 113) comment, who "understands the combined software and IT needs and necessary architectures and technology stack? Not many. Business leaders know the value chain but don't bother about technology. Manufacturing shies away when confronted with software technology. IT departments tend to overlook in their big and distant perspective that there are real products and customers. Engineering departments focus on system development and embedded electronics, and consider IT one of those big things that never work as expected. IoT … solutions must connect heterogeneous communities to understand and work together." Many of the requisite labour skills may be accessed remotely, both geographically (e.g. from labour based in different countries) and organizationally (e.g. through consultancy firms). But some of the requisite labour services will depend upon firm-specific knowledge, and this knowledge will need to be internalized within lead firms.

[4] Much of the literature has focused on the threat to jobs from the deployment of the IoT (and other digital technologies), on the potential for employee monitoring, and on privacy issues. But, as with all new technologies, there will also be new job opportunities.

A fourth constraint relates to the possibility of opportunistic behaviour by GVC participants, particularly in disaggregated value-chains, due to asymmetries of information. Birkel & Hartmann (2019) suggest that trust is a key prerequisite of successful IoT deployment. IoT adoption generates huge amounts of data on various aspects of all GVC activities, and trust will be an essential and necessary prerequisite for information sharing (Das & Teng, 1998; Falkenreck & Wagner, 2017). However, trust and optimal information exchange between independent business entities are hard to achieve, especially in the context of relationships which involve interdependencies and/or competition. Birkel & Hartmann (2019) emphasize "the importance of communication, commitment and trust in relationships, as well as credibility, and illustrate the high social., network-related and technological requirements IoT applications have to unify." The implementation of blockchain-based systems could potentially improve situations where trust is lacking between GVC participants that need to share information[5].

Last but not least, there are a range of issues related to security and privacy. The IoT involves a global network of smart, connected products collecting and processing information, and then communicating that information in real-time to people and other products. Much of this information will be commercially valuable, and some may be private and/or sensitive. This creates an imperative for robust security features to safeguard trust and privacy at all levels in the technology stack, and to prevent unauthorized access. This will require powerful authentication procedures and control of access procedures, secure storage of data, and protection from hackers (Porter & Heppelmann, 2014; Flyverboom et al., 2019). The sheer scale and scope of the IoT increase the possibilities for security lapses, especially when some activities are carried out in disaggregated value chains by participants with poor security

[5] The Trusted IoT Alliance is developing an open-source standard for integrating blockchain and the IoT (Küpper et al., 2019).

protection and in developing countries with weak data protection and privacy laws. As Bughin et al (2015: 8-9) comment, the "prospect of implementing the Internet of Things should prompt even greater concern about cybersecurity among executives. IoT poses not only the normal risks associated with the increased use of data but also the vastly greater risks of systemic breaches as organizations connect to millions of embedded sensors and communications devices. Each is a potential entry point for malicious hackers, and …. the same interoperability that creates operational efficiency and effectiveness also exposes more of a company's units to cyber-risks." Furthermore, new data protection laws and/or stronger industry self-regulation will need to be formulated to safeguard the privacy of individuals, and to put limits on what data can be accessed, stored and transmitted both nationally and across borders (Weber, 2010; Weber, 2013; Rose et al., 2015).

Implications for International Business Theory

Location and control in IoT-enabled GVCs

The contemporary global economy is based on increasingly complex global value chains (GVCs) in which value-adding activities are more geographically-dispersed and/or organizationally-fragmented than in previous years (Strange & Humphrey, 2018). Some of these GVC activities may be internalized within multinational enterprises (MNEs) but there are also manifold instances, across a range of industrial sectors including footwear, garments, toys, pharmaceuticals, vehicles and electronics, of the externalization (outsourcing) of many activities (UNCTAD, 2011). These developments have given rise to concepts such as the *global factory* (for example, Buckley & Ghauri, 2004; Buckley, 2009b; Buckley, 2011; Buckley & Strange, 2015), *factoryless goods producing firms* (Bayard, Byrne & Smith, 2015; Bernard & Fort, 2015; Morikawa, 2016), *manufacturers without factories* (Gereffi, 1999), and the *global network organization* (Pedersen, Venzin, Devinney & Tihanyi, 2014). In seeking to explain these phenomena, the IB literature has highlighted the issues of location and control (Buckley & Strange, 2015): i.e. where the GVC activities are situated within the world, and how (and by whom) these dispersed activities are coordinated. This control/governance issue has important profound implications for the capture of the rents/profits earned in the GVCs, and hence for the global distribution of income.

As regards the issue of location, the deployment of the IoT should facilitate the wider geographic dispersion of GVC activities within the global economy. Not only will the transaction costs associated with the (international) movement of intermediate goods and services be reduced, but it will also be easier to reach and obtain feedback from users worldwide. However, the realization of this ideal scenario will depend upon the constraints being non-binding. But it is likely that 5G connectivity will be limited to major cities even in advanced countries for some years, let alone in rural areas and developing/emerging countries. Furthermore, it is highly unlikely that architecture standards will be harmonized across countries, that data retention issues will be standardized, or that all countries/firms will enjoy similar levels of cyber-security. The additional costs associated with these limitations may well militate against the location of selected GVC activities in some developing/emerging countries, even if such countries potentially enjoy production costs advantages.

As regards the control issue, Brody & Pureswaran (2015: 37) claim that IoT deployment will "make the physical world every bit as easy to search, utilize and engage with as the virtual world" and hence create liquid, transparent marketplaces for physical goods. The IoT will thus facilitate the integration of GVCs, apparently without the need for lead firms providing coordination. Rifkin (2014) goes further and has even suggested that IoT deployment will lead to the death of private ownership and the eclipse of capitalism. He predicts that the "distributed, peer to peer nature of the Internet of Things platform allows millions of small players - social enterprises and prosumers - to come together in a global Collaborative Commons, erecting lateral economies of scale that eliminate the remaining middle men on the vertically integrated value chain, collapsing the mark-ups that kept marginal costs high in the past. In the coming era, everyone becomes a prosumer, producing and sharing energy and physical goods and services more directly with one another, on the Internet of Things, at near zero marginal cost and for nearly free, just as we've done in producing and sharing information goods on the Internet. This fundamental technological transformation in the way economic activity is organized and scaled portends a great shift in the flow of economic power from the few to the multitudes and the democratization of economic life." These optimistic – even utopian – predictions essentially view the IoT simply as a mechanism for transmitting information and hence improving efficiency throughout the GVC, and assumes that the information is a public good. The additional value created is thus assumed to be distributed equitably among the GVC participants, including the end users.

But the reality is that IoT deployment will require all GVC participants to develop new capabilities, will significantly alter the nature of the power relationships between the GVC participants, and will reshape competition within industries. As Porter & Heppelmann (2014: 68-69) emphasise, "Building and supporting the technology stack for smart, connected products requires substantial investment and a range of new skills - such as software development, systems engineering, data analytics, and online security expertise." These skills will involve *inter alia* capabilities in product design, after-sales service, human resources, security, and marketing. Data will be generated in real-time and will – together with people, technology and capital – become a core asset of the firm (Porter & Heppelmann, 2015). In particular, smart, connected products allow firms to develop much closer relationships with their end-users and to customize their products for individual users; this will improve user experience and allow firms to practice price discrimination at the expense of consumer surplus. Furthermore, new entrants will face significant barriers to entry, starting with the high fixed costs associated with more developing new and more complex product designs, embedding smart and connectivity components, and multiple layers of IT infrastructure.

One of the key theoretical issues in international business research is to identify the conditions under which value-adding activities within global value chains (GVCs) are best internalized within a hierarchical form of organization – i.e. the multinational enterprise (MNE) – and when activities are best externalized to independent GVC participants. Internalization theory (Buckley & Casson, 1976; Rugman, 1981; Hennart, 1982) highlights the relative benefits and costs of coordinating geographically-dispersed activities within a vertically-integrated enterprise rather than externally through the market. Thus Buckley & Casson (1976) stress that the production of most products involves a range of interdependent activities, which are connected by flows of intermediate goods and services. These intermediate goods and services include not only semi-processed materials, but also various types of knowledge (R&D, marketing etc.) and expertise embodied in human capital, patents and other intangible assets. Buckley & Casson (1976) suggest that the markets for these intermediate goods and services typically suffer from various transactional market imperfections, particularly when the activities are located in different countries. These imperfections arise from the costs of searching for, and negotiating contracts with, potential partners; buyer uncertainty about the value and nature of inputs; the costs of broken contracts, and litigation; the need to protect product quality and reputation; the absence of futures markets; inability to engage in practices such as transfer pricing and cross-subsidization, or to take advantage of government interventions, differential tax rates and exchange rate movements. These imperfections are particularly important in the markets for knowledge-based resources and capabilities, where there is an incentive to forego any form of arm's length arrangement and instead bring these activities under common ownership within an MNE. It should, however, be stressed that there are also internal transaction costs associated with organizing activities within integrated MNEs.

These internal transaction costs include the costs of acquiring and transmitting information; the costs of communication about complementary actions or of providing for them to be combined; and the costs of incentive schemes to align the actions of the members of the firm with the objectives of the firm (Buckley & Strange, 2011). The chosen governance structure will depend upon a comparison of the internal transaction costs and the market transaction costs, and the MNE will emerge as the efficient outcome if the internal transaction costs are less than the market transaction costs.

The theory predicts that lead firms will want to internalize knowledge-based assets and capabilities, as this will enable them to control their GVCs and the distribution of the value-added generated therein. In IoT-enabled GVCs, these assets and capabilities will be those related to product design and development, data analysis, and operating and maintaining the technology stack. In contrast, the theory predicts that lead firms will want to externalize the sourcing of standardized intermediate products which do not require transaction-specific investments, and for which measurement and monitoring costs are low (Strange & Humphrey, 2018). IoT deployment will reduce these measurement and monitoring costs still further especially when the intermediate products are made in foreign countries. Markets for standardized intermediate products will become thicker (McLaren, 2000) as more suppliers become connected, the products will become commoditized, and this will drive down prices as activities are offshored to cheaper foreign locations. Thus, internalization theory predicts that IoT deployment will facilitate the externalization of standardized intermediate products, whilst encouraging lead firms to internalize the valuable activities listed above. Rather than the democratization of economic life and a shift in economic power from the few to the multitudes as a result of IoT deployment, the opposite will be the case. Power asymmetries will be exacerbated, and ever greater shares of the value created within GVCs will be captured by lead firms with capabilities in product design and development, data analysis, and operating and maintaining the technology stack. Many of these lead firms, though not all, will be located in countries which possess the necessary human resources and technology, and this is likely to be the advanced countries. This conclusion also emphasises the need for all countries to address local constraints to IoT deployment, as otherwise they will certainly miss out on the benefits of IoT deployment.

IoT-enabled innovation ecosystems

Much of the popular attention to date has been devoted to consumer applications of the IoT, such as connected household appliances (Osmonbekov & Johnston, 2018). But the potential for business-to-business applications, as argued, should be rather greater, with sensors able to provide real-time data *inter alia* to gather and make sense of consumer data and to deliver the right kinds of products and services at the right time (Windpassinger, 2017), to monitor inventory levels and allow better capacity planning, to detect equipment wear-and-tear and thus permit preventative maintenance, and to assess the usage and functionality of products (Bughin *et al.*, 2015). This will necessitate a greater integration of data between lead firms, suppliers and customers, and a reduction in the need for intermediaries. Fleisch (2010: 6-7) even suggests that in "an ideal open IoT-architecture, not only can every sensor be reached by every authorized computer or person, but in addition, every person and organization can set up their own services, link them with identifiers, and offer them to the public. For instance, a tag on a consumer good would not just provide a link to the product homepage provided by the producer… [but] it would generate an additional list of alternative services provided by independent firms or not-for-profit organizations from which the user or the user's computer system can choose. This list could include services such as product rating, fair trade check, counterfeit check, proof-of-origin, replenishment alert, political shopping, … or self check-out."

An often-underexplored firm-level capability in the international business literature relates to demand-side innovation (Priem et al., 2012); that nonetheless will play a crucial role in realizing the benefits of the IoT. The data collected by sensors and analyzed by the IoT platform may be used to discover latent demand-side preferences and accordingly provide alternative services, but not necessarily by the lead firm itself (Fleisch, 2010). This will have two important implications. First, the power asymmetry between the GVC participants may be yet again exacerbated. The physical product itself will be increasingly commodified whilst value accrues more from the services that address the very customer preferences discovered by data analytics (Porter & Heppelmann, 2014). Since service innovation capabilities are primarily clustered in advanced countries and the agglomeration economy is unlikely to dissolve in the short term, firms' capacities to capture value will remain distributed geographically unevenly. It may be even more so given that the delivery of value propositions is largely digitised. Put differently, delivering IoT-supported services to foreign customers does not require as much country-specific institutional knowledge and asset exposure, which will only amplify the advantages of advanced country firms.

Second, the vast heterogeneity in global demand preferences (Zhang et al., 2019) suggest that the lead firm may operate an open system where third-party, autonomous innovators are encouraged to join and develop alternative, complementary service applications based on the data collected and shared. These services do not have to be aligned with the primary interests of the lead firm, yet rather aim to serve unmet demands outside the lead firm's domain of expertise. Such an organizing structure is based on the principle of co-specialization, as predicted by the theory of the ecosystem (Jacobides et al., 2018). Governing the relationships with and among these autonomous innovators may involve neither arm's length transaction nor internalization (Banalieva & Dhanaraj, 2019). Instead, the modular architecture of the IoT allows the lead firm to orchestrate an ecosystem involving a multilateral set of interdependent

GVC participants. The relationship between the lead firm and each GVC participant is based on modular design principles and does not require dyadic negotiation of transactional contracts (Li et al., 2019). So long as there exists complementarity in production and/or consumption, different third-party components—linked by the sensor or its data flow—can be recombined by various users due to interoperability. Meanwhile, it does require ecosystem-specific investment by these autonomous innovators, not least because of the varying architecture standards discussed earlier. Hence the divide in standards emerging in the Sino-US technology race may well impair the potential of IoT-driven industrial ecosystems and the associated productivity gains.

Concluding Remarks

The next few years are likely to witness the widespread adoption of the IoT and a proliferation not only of smart consumer products but also of business applications. In terms of business applications, many commentators have already highlighted the potential benefits in terms of the greater operational efficiency of supply chains, preventative maintenance, and the collection and analysis of user feedback, as well as the provision of a more personalized experience for users/consumers. The basic elements required for the IoT technology stack (i.e. devices, gateways, service platforms) are already commercially available, and their deployment awaits the roll-out of fifth-generation (5G) telecommunications technology.

From an IB theory perspective, the first key issue relates to how IoT deployment will affect the location of activities within global value chains (GVCs). Our understanding is that 5G connectivity (or the lack of it) will play a vital role in determining where activities are located, and the lack of connectivity may well limit the attractiveness of many developing and/or emerging countries and rural areas. This raises policy considerations about potential subsidies by host country and regional governments. Other important factors are likely to be concerns about security and data protection. The second key issue relates to how the value created by IoT deployment in GVCs is captured, how it is distributed, and by whom (Porter & Heppelmann, 2014). We are sceptical that the value will be distributed equitably in a global collaborative commons, but envisage that GVC participants will vie to capture disproportionate shares of the rents generated (Strange & Humphrey, 2018). More specifically, we envisage that lead firms will try to internalize key resources and capabilities within their IoT-enabled GVCs so as to exercise control and leverage the power asymmetries. These resources and capabilities will be those related to certain labour services (systems engineering, machine learning, software design, data analytics etc) required to customize and optimize IoT systems, and to collate and analyse the product-related information that is generated. Furthermore, trust is a necessary prerequisite for information sharing. In the absence of mechanisms to provide such trust, lead firms may opt to internalize information flows. In short, knowledge will be increasingly internalized, while operations are increasingly externalized (Liebeskind, 1996; Buckley & Strange 2015). Meanwhile, in creating greater value for customers, the lead firm is incentivized to allow autonomous innovators to develop alternative service applications. One might expect that firms in the GVC will coalesce into IoT-based ecosystems around the lead firm, involving neither transaction negotiation nor internalization. Yet, one must also note that the ecosystem's full potential could be impeded by the standards divide between major economies. IoT deployment is still in its infancy, but many commentators confidently predict that there will be an explosion in the numbers of smart, connected products in the coming years. This eventuality will enable researchers to investigate empirically our predictions, and also to measure the scale of the benefits that are generated by IoT adoption.

References

Banalieva, E. R., & Dhanaraj, C. (2019). Internalization theory for the digital economy. *Journal of International Business Studies*, 50(8): 1372-1387.

Bhatia A., Yusuf, Z., Misra, N., Andersen, P., White, J., Nandi, S., Subramania, J. & Bhat, N. (2019). *Beyond predictive maintenance: the 'art of the possible' with IoT*. Boston Consulting Group.

Birkel, H.S. & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply chain management: an international journal.*,

Brody, P. & Pureswaran, V. (2015). The next digital gold rush: how the internet of things will create liquid, transparent markets. *Strategy & Leadership*, 43(1): 36-41.

Buckley, P.J. & Casson, M.C. (1976). *The future of the multinational enterprise*. London: Macmillan.

Buckley, P.J. & Strange, R. (2011). The governance of the multinational enterprise: insights from internalization theory. *Journal of Management Studies*, 48(2): 460–470.

Buckley, P.J. & Strange, R. (2015). The governance of the global factory: location and control of world economic activity. *Academy of Management Perspectives*, 29(2): 237-249.

Bughin, J. Lund, S. & Manyika, J. (2015). Harnessing the power of shifting global flows. *McKinsey Quarterly*, February, pp.1-13.

Capri, A. (2018). Beijing's global 5G ambitions threaten to disrupt telecoms. *Nikkei Weekly*, 31 August.

Chen, H., Chiang, R.H.L & Storey, V.D. (2012). Business intelligence and analytics: from big data to big impact. *MIS Quarterly*, 36(4): 1165-1188.

Chiaraviglio, L., Blefari-Melazzi, N., Liu, W., Gutierrez, J.A., van de Beek, J., Birke, R., Chen, L., Idzikowski, F., Kilper, D., Monti, P., Bagula, A. & Wu, J. (2017). 5G in rural and low-income areas: is it feasible?' *IEEE Communications Standards Magazine*, 1(4): 50–57.

Coviello, N., Kano, L., & Liesch, P.W. (2017). Adapting the Uppsala model to a modern world: Macro-context and microfoundations. *Journal of International Business Studies*, 48(9): 1151-1164.

Das, T.K. & Teng, B-S. (1998). Between trust and control: developing confidence in partner cooperation in alliances. *Academy of Management Review*, 23(3): 491-512.

De Cremer, D.D., Nguyen, B. & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side. *Journal of Marketing Management*, 33(1-2): 145-158.

Ehret, M. & Wirtz, J. (2017). Unlocking value from machines: business models and the industrial internet of things. *Journal of Marketing Management*, 33(1-2): 111-130.

Falkenreck, C. & Wagner, R. (2017). The internet of things: chance and challenge in industrial business relationships. *Industrial Marketing Management*, 66: 181-195.

Fleisch, E. (2010). *What is the Internet of Things? An economic perspective*. Auto-ID Labs, White Paper WP-BIZAPP-053.

Flyverboom, M., Deibert, R. & Matten, D. (2019). The governance of digital technology, big data, and the internet: new roles and responsibilities for business. *Business & Society*, 58(1): 3-19.

Gupta, M & George, J.F. (2016). Toward the development of a big data analytics capability. *Information & Management*, 53(8): 1049-1064.

Hennart, J-F. (1982). *A theory of multinational enterprise*. Ann Arbor: University of Michigan Press.

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, 39(8): 2255-2276.

Kenney, M. & Zysman, J. (2018). Work and value creation in the platform economy. University of California Berkeley, Berkeley Roundtable on the International Economy (BRIE) Working Paper 2018-4.

Küpper, D., Ströhle, J., Krüger, T., Burchardi,K. & Shepherd, N. (2019). *Blockchain in the factory of the future*. Boston Consulting Group.

Leminen, S., Rajahonka, M., Westerlund, M. & Wendelin, R. (2018). The future of the Internet of Things: toward heterarchical ecosystems and service business models. *Journal of Business & Industrial Marketing*, 33(6): 749-767.

Liebeskind, J.P. (1996). Knowledge, strategy, and the theory of the firm. *Strategic Management Journal*, 17(S2): 93-107.

Li, J., Chen, L., Yi, J., Mao, J., & Liao, J. (2019). Ecosystem-specific advantage in international digital commerce. *Journal of International Business Studies*, forthcoming.

Lu, Y., Papagiannidis, S. & Alamanos, E. (2018). Internet of things: a systematic review of the business literature from the user and organisational perspectives. *Technological Forecasting and Social Change*, 136: 285-297.

McLaren, J. (2000). Globalization and vertical structure. *American Economic Review*, 90(5): 1239-1255.

Osmonbekov, T. & Johnston, W.J. (2018). Adoption of the Internet of Things technologies in business procurement: impact on organizational buying behaviour. *Journal of Business & Industrial Marketing*, 33(6): 781-791.

Porter, M.E. & Heppelmann, J.E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, 92(11): 64-88.

Porter, M.E. & Heppelmann, J.E. (2015). How smart, connected products are transforming companies. *Harvard Business Review*, 93(10): 97-114.

Priem, R. L., Li, S., & Carr, J. C. (2012). Insights and new directions from demand-side approaches to technology innovation, entrepreneurship, and strategic management research. *Journal of Management*, 38(1): 346-374.

Rifkin, J. (2014). The zero marginal cost society: the internet of things, the collaborative commons and the eclipse of capitalism. *The World Financial Review*, 30 June.

Rose, K., Eldridge, S. and Chapin, L. (2015). *The internet of things: an overview. Understanding the issues and challenges of a more connected world*. The Internet Society (ISOC).

Rüβmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P. and Harnisch, M. (2015). *Industry 4.0: the future of productivity and growth in manufacturing industries*. Boston Consulting Group.

Rugman, A.M. (1981). *Inside the multinationals: the economics of the multinational enterprise*. New York: Columbia University Press.

Strange, R. & Humphrey, J. (2018). What lies between market and hierarchy? Insights from internalization theory and global value chain theory. *Journal of International Business Studies*, forthcoming.

Strange, R. & Zucchella, A. (2017). Industry 4.0, global value chains and international business. *Multinational Business Review*, 25(3): 174-184.

Vella, H. (2019). 5G vs 4G: what is the difference?' *Raconteur*, 15 May.

Weber, R.H. (2010). Internet of things: new security and policy challenges. *Computer Law* and *Security Review*, vol.26, no.1, pp.23-30.

Weber, R.H. (2013). Internet of things: governance quo vadis?' *Computer Law* and *Security Review*, vol.29, no.4, pp.341-347.

Weyrich, M. & Ebert, C. (2016). Reference architectures for the Internet of things. *IEEE Software*, January-February: 112-116.

Windpassinger, N. (2017). *Internet of things: digitize or die*. IoT Hub.

Woodside, A.G. & Sood, S. (2017). Vignettes in the two-step arrival of the internet of things and its reshaping of marketing management's service-dominant logic. *Journal of Marketing Management*, 33(1-2): 98-110.

Zhang, X., Xie, L., Li, J., & Cheng, L. (2019). "Outside in": Global demand heterogeneity and dynamic capabilities of multinational enterprises. *Journal of International Business Studies*, forthcoming.

Zucchella, A., Strange, R. & Cerrato, C. (2019). Digital transformation and the international strategy of the firm: how digital technologies affect the international marketing approach in the footwear industry. Paper presented at the LUMSA Conference on *Digital Transformation and Internationalization of Firms: Prospects, Challenges and Future Agenda*. Palermo, February.

Figure 1: The Technology Stack